EACH
European Association of CCP Clearing Houses

EACH Paper

CCP Core Cyber Incident Handling Principles

May 2024

Executive Summary

Given the current threat landscape, with a continuous and increasing number of large scale and disruptive cyber-attacks in different industries across the world, EACH members have put together a set of Core Central Counterparty (CCP) Principles for Cyber Security. These principles provide clearing members, settlement institutions, vendors, regulators and other interested parties a view on how EACH Members conduct the principles of Response, Recovery and Reconnection:

1. **Response**: Preparing for and coping with the immediate impact of a breach, including:
    - Ensuring proper response planning for a variety of scenarios.
    - Ensuring appropriate communication during an incident.
    - Analysis and mitigation of the threat via the appropriate plan.
    - Incorporating any lessons learned.

2. **Recovery**: Subsequently rebuilding and restoring of ICT systems, including:
    - Ensuring proper planning for recovery situations and use of plans when required.
    - Ensuring appropriate communication during the recovery phase.
    - Incorporating any lessons learned from incidents and testing.

3. **Reconnection**: Reconnecting to market infrastructures, service providers and other organisations, including:
    - Ensuring proper policies for reconnection to the impacted system, for when the vulnerability has been identified and remediated.
    - Ensuring communication during the reconnection phase
    - Incorporating any lessons learned from incidents and reconnection tests.

These principles are known as the ‘3Rs principles’ and are complementary to the CCP’s own risk management processes and cybersecurity programs. Any lessons learnt from previous cyber-attacks or experiences shared by other affected or victim CCPs are to be used by EACH members to update their Response, Recovery and Reconnection strategies. EACH members also emphasise the importance of performing of regular testing exercises to improve their ability to uncover gaps, thereby ensuring optimal preparedness for upcoming threats.

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of CCPs in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient, and transparent global financial markets. EACH currently has 18 members from 14 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

Cyber-attacks such as ransomware attacks continue to threaten the financial industry[1] with attackers continuously evolving and expanding their capabilities resulting in cyber incidents becoming increasingly complex to respond to, and with an increasingly broader business and market impact.

Maintaining high levels of cyber hygiene and continuous improvements of operational resilience remains of the highest priority for CCPs: the ever evolving and rapidly changing cyber threat landscape as well as the associated material breaches within it over the past 10 years have clearly illuminated that no one is immune to cyber breaches regardless of the preventative efforts that may have been taken to avoid them. As such, preparedness for the immediate response to and continued longer term handling of a cyber breach is hugely important.

Furthermore, CCPs are amongst other already highly regulated entities and are required to comply with all existing rule and regulations which importantly contain information security/cyber security requirements, and which ultimately aim to protect the global financial markets. By complying with such regulations, CCPs establish appropriate internal controls that maintain a high level of technology and cyber hygiene to protect from the diverse and complex range of cyber-attacks that exist in today's cyber threat landscape.

This paper describes the core cyber incident handling principles that European CCPs consider when implementing, maintaining and enhancing the effectiveness of their controls associated with cyber incident **Response**, **Recovery** and **Reconnection.**[2]

[1] See for example the cyber-attack on ION in January 2023: https://www.ft.com/content/35b357f6-bbb9-46b1-9b46-34bc2d60eb75.

[2] In alignment with FIA_Taskforce on Cyber Risk_Recommendations_SEPT2023_Final2.pdf.

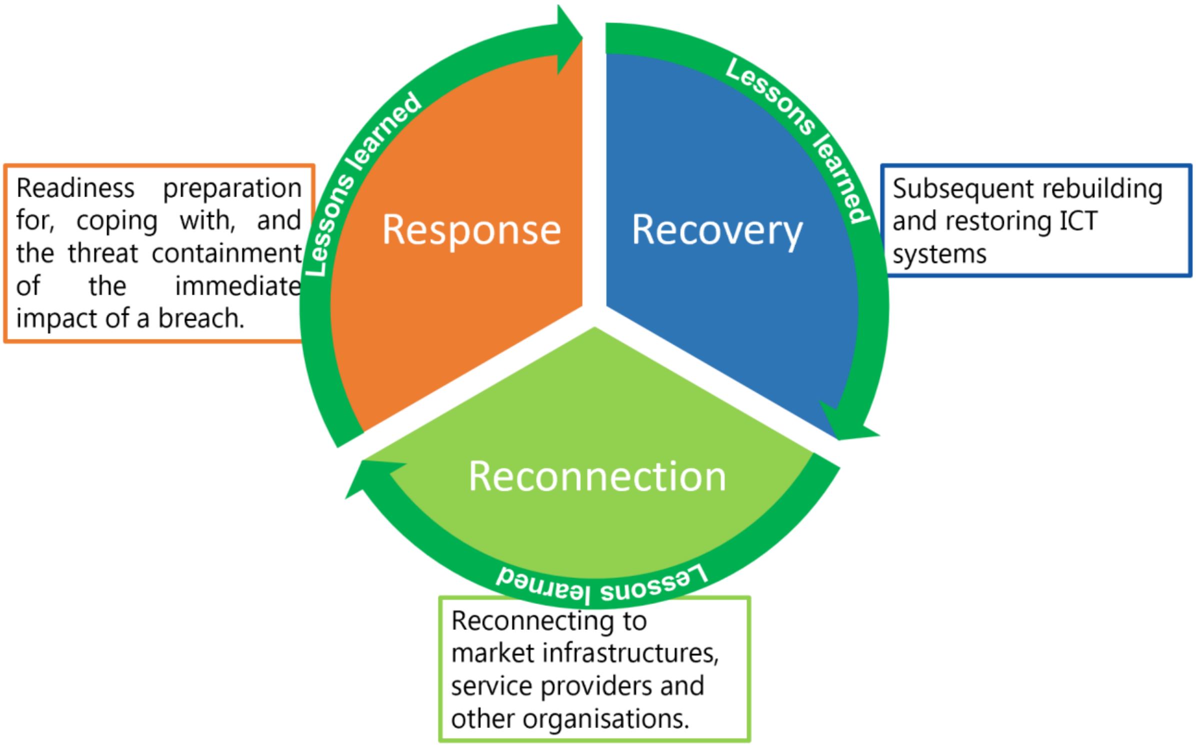
Readiness preparation for, coping with, and the threat containment of the immediate impact of a breach.
Lessons learned
Response
Recovery
Lessons learned
Subsequent rebuilding and restoring ICT systems
Reconnection
Lessons learned
Reconnecting to market infrastructures, service providers and other organisations.

Figure 1: Overview of the Response, Recovery and Reconnection phases.

The application of Response, Recovery and Reconnection (Figure 1) is considered as complementary to the CCPs' own risk management processes and cybersecurity programs which are in line with existing frameworks/rules[3], and are typically aligned in their implementation with the common aspects and universal principles defined within, but not limited to, elements such as the following:

- *Framework for Improving Critical Infrastructure Cybersecurity* established by the *National Institute of Standards and Technology* (NIST)[4],
- *Principles for Financial Market Infrastructures* (PFMI) (CPMI-IOSCO)[5],
- *Cross Market Operational Resilience Group* (CMORG)[6],
- *European Market Infrastructure Regulation* (EMIR)[7],
- *Digital Operational Resilience Act* (DORA)[8].

EACH members are committed to learning from their own previous cyber events and incidents, or similar experiences shared by other affected victims in the financial industry or from Special Interest Groups (SIGs) such as Financial Services Information Sharing and Analysis Center (FS-ISAC), National Cyber Security Center (NCSC), Interpol, etc. CCPs consider lessons learned hugely important in the process of improving operational resilience and use them to update their Response, Recovery and Reconnection strategies and internal control processes. EACH

[3] Such as CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, ISO/IEC 27002, EBA guidelines in ICT and security risk management. Please note the list is non-exhaustive.
[4] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov).
[5] PFMIs
[6] Cross Market Operational Resilience Group (CMORG).
[7] European Market Infrastructure Regulation (EMIR) here.
[8] Digital Operational Resilience Act (DORA) here.

members continuously improve their ability to identify control gaps or weaknesses and vulnerabilities, thereby ensuring optimal preparedness to deal with cyber threats and attacks. CCPs encourage the execution cyber scenario-based exercises to ensure that their incident handling teams are aware of their responsibilities and functional roles during a cyber event/incident.

Additionally, EACH members believe that the continuous process of improving organisation-wide awareness and responsibilities around identifying and reporting cyber incidents (or potential incidents) for all staff, done amongst other through initiatives such as phishing campaigns, interactive knowledge sessions, internally published knowledge articles, and mandatory security trainings such as high-risk user trainings are also key in the fight against cyber-threats.

To ensure that this paper remains relevant and aligned to the current cyber threat landscape, it will be reviewed, and where necessary, updated on a regular basis.

1. Response – Coping with the immediate impact of a breach

Response refers to readiness preparation for and coping with the immediate impact of a breach. The principles covered in Response are:

- To ensure proper response planning for a variety of scenarios and communication in an incident with internal and external stakeholders;
- To analyse and mitigate the threat, and
- To incorporate the lessons learned from incidents and testing into the relevant plans and frameworks.

a) Response Planning

In a cyber incident, it is crucial for any organisation to have a regularly tested incident response plan, as any uncoordinated action and subsequent delay or confusion during the incident handling may lead to an erosion of trust in the market. Therefore, it is essential to be able to respond swiftly to a cyber incident's scale, speed and propagation for example by making use of scenario-based playbooks. The level of preparedness is key to define a coherent and thus more effective response to a cyber incident. This is also why CCPs have documented incident response plans that outline different phases of incident management and define roles and responsibilities for their incident handling teams. Such a response plan is well complemented by elements such as cyber playbooks and business continuity plans that cover cyber.

The response plans that CCPs establish are a roadmap for their individual incident response framework for defining short and long-term goals and are executed according to the severity of the incident. It is important that the response plan is simple and very clear to be implemented effectively so that incident handling teams can easily follow the plan and act in a coordinated way in the pressured and stressed environment of a real cyber incident. CCPs aim to continuously maintain their response processes and procedures to be able to respond effectively to cybersecurity incidents.

Additionally, for effective execution of response plans, CCPs advocate planning and conducting routine cyber scenario themed exercises for the assigned incident handling teams. These serve the purpose of maintaining awareness and training these teams in responding to real world threats from the current cyber threat landscape. Such testing exercises cover different scenarios including worst-case and extreme but plausible scenarios and are conducted on a regular basis.

b) Communications

Communication with both internal[9] and external stakeholders is key in an ongoing cyber incident. CCPs aim to supply their stakeholders with accurate and transparent information in

[9] These include for example incident handling teams, media relations, regulatory officers, executive and supervisory board, and staff.

a manner that does not place the active investigations that are underway at risk.[10] Communication plans ensure that incident handling teams know their responsibilities when a response is needed and that coordination with external stakeholders occurs consistently in accordance with the response plan. They also include details about who to communicate with internally and who is authorised to communicate. This should also reduce information irregularities between different position keepers and achieve broader situational awareness.

Furthermore, EACH members support the principle of having inter-CCP communication and information sharing in the case of a cyber incident and on the principle of facilitating information sharing between CCPs. For transparency reasons, decisions and actions taken are communicated as appropriate between stakeholders such as the victim CCP, intra-group entities, its reconnecting members, vendors, regulators and law enforcement. Following the event, incident debrief and lessons-learned provide an opportunity to learn and adjust as required.

c) Analysis

If a CCP becomes a cyber-attack victim and has commenced its response, it initiates a defined documented incident response plan which may leverage other established cyber scenario playbooks including analysis to ensure effective response activities. It is important that after forensic investigations are performed and when they deem it appropriate to do so, the impact and source of the incident are clearly communicated by the compromised CCP with a focus on operations, technology, data, transactions, customer, partners such as third parties or vendors and payment systems.[11] Severity and nature of incidents are categorised and documented consistent with the CCP's response plan, to determine the appropriate mitigation and recovery strategy. EACH members strongly encourage developing scenario playbooks to help with response activities and recovery/solution strategies. This includes systems and infrastructure services that support important business services which have been identified beforehand and allow incident handling teams to determine which systems must be recovered first.

d) Mitigation

In the case of an incident, activities are performed by the compromised CCP to prevent expansion of an event, mitigate its effects, and resolve the incident. It is essential that incidents are contained and mitigated in a uniform and controlled approach. Overall, CCPs intend to take all steps necessary to discover the root cause of the attack (see section c) analysis above and implement measures aimed to effectively contain damage and radius as quickly as possible, further eradicating the presence of the attacker with the aim of eventually restoring the integrity of remediated systems.

e) Lessons Learned

Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. CCPs work towards incorporating such lessons

[10] These include for example critical vendors and service providers, clients and partners that connect to the CCP's network, legal and regulatory institutions (e.g., ESMA, the CCP's applicable Data Protection Authority (DPA), and the respective national Financial Supervisory Authorities (e.g., AFM, BaFin etc.).

[11] See System Integrity Reconnection Framework of CMORG.

learned into their response plans. Hence, any insights gained from past incidents are used to improve their long-term incident response strategy. Additionally, by regularly testing their response readiness, EACH members are better able to uncover gaps in their response strategies. This provides them with an opportunity to refine and improve their response plans. It should also raise awareness and support assistance in educating incident handling teams on the importance of effective cyber incidents responses.

2. Recovery – Rebuilding and restoring ICT systems

Recovery refers to the subsequent rebuilding of ICT systems after the initial cyber breach has been managed and the threat either contained or removed from the technology estate. The principles covered in Recovery are:

- To ensure proper planning for recovery situations, and using these plans appropriately if required;
- To communicate during the recovery phase and;
- To incorporate any lessons learned relating to both recovery plans and processes, resulting from both real incidents and testing.

a) Recovery Planning

Recovery processes and procedures such as disaster recovery and business continuity plans play a key role in ensuring restoration of systems affected by cyber security incidents. Therefore, EACH members aim to have recovery concepts/strategies in compliance with applicable regulations (e.g. which allow them to act accordingly and in a coordinated manner during or after being compromised). Recovery systems and back-up procedures must be compliant with relevant regulatory requirements and have the ambition level to meet highest available security standards and best practices. In addition, aiming for maximum preparedness, CCPs encourage the use of individual cyber themed playbooks with the aim of guiding a prompt recovery in the case of a cyber-attack.

b) Communication

Communication is equally important when a compromised CCP is recovering from a cyber security incident. CCPs therefore aim to consider how to coordinate any restoration activity they will perform with internal and external parties, i.e. CCPs emphasise the regular testing of their reconnection and communication plans. It is essential that after discovering and responding to the attack, the focus is to re-establish operations in a secure environment. The recovery activities are to be communicated to internal and external stakeholders when it is appropriate to do so (e.g. when relevant information is available, after internal approval, etc.)

c) Lessons learned

As it is the case for the Response phase, incorporating lessons learned from previous incidents into recovery planning and processes are essential. For a better understanding of vulnerabilities and contagion channels, it is in the interest of EACH members to continuously apply any findings from disaster recovery exercises and actual incident recoveries to established recovery plans (e.g. by post-incident review). Therefore, CCPs also aim to incorporate any lessons learned or experiences shared by other victims. EACH members deem it essential to have their recovery strategies and plans updated and maintained on a regular basis. This also means that existing business-wide incident management procedures are updated regularly by providing/incorporating procedures for cyber incidents.

3. Reconnection – Reconnecting to market infrastructures, service providers and others

Reconnection refers to the stage at which CCPs reconnect to market infrastructures, service providers and other organisations. The principles covered in Reconnection are:

- To define policies for reconnection to the impacted system, once the vulnerability has been identified and remediated;
- To ensure communication during the reconnection phase and;
- To conduct reconnection tests and incorporate any lessons learned.

a) Reconnection policies

Once the vulnerability has been responded to and the impacted system(s) of the victim CCP is recovered, the reconnection stage begins. Based on the incident description and remediation measures, the victim CCP decides when to reconnect to the systems and communicates this to clients. To this end, CCPs aim to use their own established reconnection plans, policies and playbooks that provide appropriate guidance after an incident. These include details on the technical process such as the establishment of connectivity with selected stakeholders using a phased approach, making low-value test transactions with key stakeholders, and undertaking heightened transaction monitoring across all relevant parties for the respective period. The established reconnection procedures are best applied in an orderly manner based on risk-informed principles for reconnection such as operational stability and criticality.

b) Communication

Similarly to the Response and Recovery phase, communication is also key after CCPs have applied appropriate tests to verify secure and stable reconnection and for example make use of defined roll-back plans before any reconnection attempts or activities are done and before normal operations can resume.[12]

c) Reconnection tests

Whilst reconnection implies that a cyber incident was successful to some degree, it is equally essential to test reconnection policies and plans so that one may learn from them in case of a possible real-life need to reconnect. Hence, CCPs encourage regular testing of reconnection and communication to ensure a maximum level of preparedness in the event of a successful cyber-attack. CCPs aim to align closely with regulators and other industry associations on standard approaches for such tests in order to achieve a maximum of efficiencies.

-END-

[12] See System Integrity Reconnection Framework of CMORG.